A Canadian Business Perspective on Protecting Personal Information and Ensuring Global Information Flows

Murray Long
President, Murray Long & Associates Inc.
Ottawa, Canada

The privacy Issue in Canada

- Growing consumer concern about loss of control over personal data
- Impact of lack of consumer trust on e-commerce growth
- Calls by major business organizations for consistent rules and a level playing field
- Concerns about the EU Directive

The Early Leadership of Quebec

- First North American jurisdiction to enact a private sector privacy law
- Predated the EU Directive by one year (1994 enactment)
- No perceived harm to business
- Created situation where 25 percent of Canadians had legally enforced privacy rights in the private sector

The Government Response

- New law based on CSA Code developed by business, consumer groups and other stakeholders
- One-year phase in for business subject to federal government regulation
- Four year phase in period for business subject to provincial regulation
- Four year period for provinces to enact their own laws

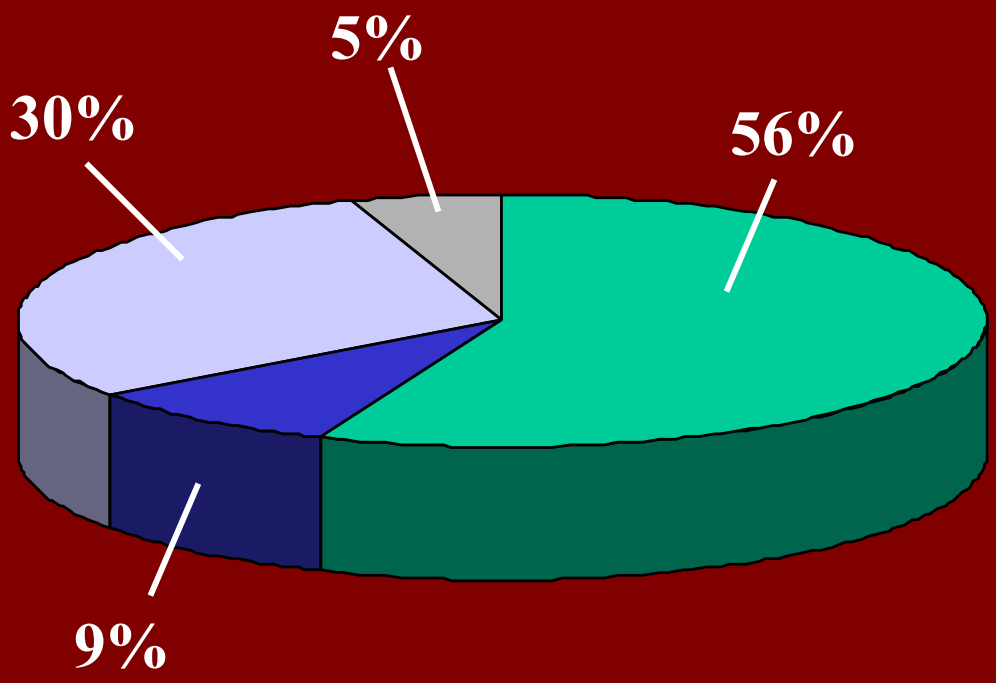
The Intent of the New Law

- Harmonized privacy standards across all jurisdictions
- Rules based on code that combines clear obligations with some flexibility to meet business needs
- Privacy Commissioner to act as ombudsman with strong investigative powers, but no order-making powers
- Federal Court stands behind the law to enforce rules where required

How well the law is Working

- More than 45,000 businesses are subject since January, 2001 - they continue to improve their practices
- There have only been 112 complaint investigations in first two years
- Commissioner investigation findings are published on his web site, without names, providing more insight into interpretation of the law

How Complaints Break Down



- Well-founded
- Partially well-founded
- Not well-founded
- Discontinued or no jurisdiction

The International Aspects

Under our law, Canadian companies must protect data travelling to and from other countries

Our law meets the EU Directive, permitting trans-border data flow

Dec. 2001 Decision by EC

Nuts and Bolts of the Law

The CSA Code embedded in the law is based on widely accepted OECD Guidelines

The language has been updated to be consumer-friendly and reflect current information use issues in private sector data collection

Oversight is complaints-driven, but the Privacy Commissioner can conduct independent investigations

All transborder data flow will always be under the federal law, even if provinces have their own laws

Benefits within Canada and abroad

- More consumer trust based on data protection rules
- More business certainty based on clear obligations and a level playing field
- Canada trusted as a country that protects personal data under law
- No need to hammer out bi-lateral or multi-lateral arrangements that only apply to some businesses

The 10 CSA Principles

- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting Use, Disclosure, or Retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance

The CSA Privacy Code is an evergreen code that must be reviewed every five years and can be updated to reflect changing requirements. The legislation is also reviewed every 5 years.

Issues with the law

- Some interpretation challenges
- One individual complaint can result in a major change in business practices
- Infusion of human rights privacy values into commercial activity
- Lack of finality in Commissioner interpretations - two interpretive complaint findings now before the Federal Court

Acceptance so Far

- No serious problems for business
- How it affects small business yet to be determined
- Business and consumers generally satisfied with outcomes

International Issues

- Need for other countries to adopt similar, enforceable privacy laws
- Global e-commerce benefits will flow to countries that have private sector privacy laws
- Our law applies to any company with a tangible business presence in Canada
- Data cannot be shipped off to other jurisdictions, without ensuring adequate data protection

Final Perspectives

- One FTC report to Congress estimates lost online retail sales due to privacy concerns may be as much as $18 billion in 2002.
- Canada's largest bank (Royal Bank Group) reported in 2002 that privacy accounts for 14% of brand value. For the Royal Bank this represents $679 million CDN that depends on privacy leadership.

What should APEC Consider?

- Common principles/values in data protection
- Careful weighing of the advantages or disadvantages of self-regulatory approaches versus a legislated approach
- the need to have mutual agreement regarding implementation
- Necessary flexibility for local markets to address local conditions